REMARKS

Claims 1-45 are pending. Claims 1, 9-10, 12, 18, 25-27, 31-32, 35, 37-38, and 44 have been amended. Claims 8, 30, 33-34, 39, and 45 have been canceled. No new matter has been added. The rejections of the claims are respectfully traversed in light of the amendments and following remarks and reconsideration is requested.

Claim Objections

Claim 18 is objected to because the acronym "MAC" should be spelled out.

Claim 18 has been amended to recite "media access controller (MAC)". Accordingly, Applicant requests that the objection to Claim 18 be withdrawn.

Rejection Under 35 U.S.C. § 102

Claims 1-17 and 19-45 are rejected under 35 U.S.C. § 102(e) as being anticipated by Sims, III (U.S. Patent No. 6,550,011 hereinafter "Sims").

In rejecting the claims, the Examiner writes in part:

> In respect to claim 1, Sims discloses a user data processor for providing access to a rights controlled data object, the user data processor comprising . . . a user program running on the processing device, the user program configured to control access to the rights controlled data object; a user program security module configured to at least partially decrypt the secure package using a user program key (see col. 9, lines 60-67); and a machine key device connected to and associated with the processing device and accessible by the user program, the machine key device configured to restrict the use of the data object to the user data processor using a machine key (see col. 15, lines 18-34).
>
> . . .
>
> In respect to claim 8, Sims discloses the user data processor of Claim 1, further comprising a user key device associated with a user, the user key device detachably connected to the processing device, accessible by the user program, and configured to restrict the use of the data object to the user using a user key (see col. 9, lines 60-67 and col. 11, lines 5-15).

v1

-11-

Serial No. 09/760,956

However, Sims discloses the following:

> Additionally or alternatively, it is also possible to uniquely <u>encrypt</u> the content per user so that if unauthorized copies are made available or a secret key is published <u>the source</u> might be identified. However, use of multiple content keys for a single protected work increases costs in that multiple keys must be generated and maintained as well as multiple pr[o]cessing of the content to <u>encrypt</u> it must be accomplished. (Sims, col.9, lines 60-67) (emphasis added).

> An <u>information use device</u>, such as <u>use devices</u> 111 and 112, preferably a standalone secure unit, such as a secure component of a computer system (e.g. computer 101) or a "tamper resistant" software component of a computer system (either of which may be represented by user device 111) or an independently operable device such as a portable player (which may be represented by user device 112). Accordingly, the preferred embodiment user device includes a processor (processor 114) and associated instruction set to control operation of the <u>use device</u> and its components according to the present invention. (Sims, col.11, lines 5-15) (emphasis added).

Thus, Sims only discloses <u>encryption</u> of content "per user" and examples of an information <u>use device</u> in the sections referenced by the Examiner above. As shown in Sims, column 8, line 67, reference is made to "use devices 111 and 112. A "user" device 111 or 112 appears to be a typographical error. Even if not a typographical error, Sims does <u>not</u> disclose or suggest decryption or use restriction of a data object to <u>a particular user</u> and <u>a particular data processor</u> based upon a user key and a machine key or authentication thereof. Sims also does not disclose or suggest a detachably connected user key device.

In contrast, amended Claim 1 recites a data processor, comprising "a user key device associated with a user, the user key device <u>detachably connected</u> to the processing device, accessible by the user program, and configured to <u>restrict the use of the data object to the user using a user key</u>" and "a machine key device connected to and associated with the processing device and accessible by the user program, the machine key device configured to <u>restrict the use of the data object to the user data processor using a machine key</u>."

Similarly, amended Claim 25 recites a method, comprising "encrypting the data object such that <u>decryption requires the user program key and the machine key</u>" and "encrypting the data object such that <u>decryption also requires the user key</u>."

Similarly, amended Claim 32 recites a method, comprising "creating a machine control element configured to cause the user program to restrict use of the data object to the

v1   -12-   **Serial No. 09/760,956**

particular user data processor by authenticating the particular user data processor based upon at least the machine key and by at least communicating with the machine key device" and "creating a user control element configured to cause the user program to restrict use of the data object to the particular user by authenticating the particular user based upon at least the user key and by at least communicating with the user key device."

Similarly, amended Claim 38 recites a method, comprising "encrypting the data object such that decryption requires the user program key and the machine key", "decrypting the data object using the user program key and the machine key", "encrypting the data object such that decryption also requires the user key", and "decrypting the data object using the user key."

Similarly, amended Claim 44 recites "a secure data package . . . comprising a controlled portion of the data object, the controlled portion encrypted such that decryption requires both a user program key and a machine key, . . . wherein the controlled portion is additionally encrypted such that decryption requires a user key, wherein the user key is maintained by a user key device associated with a particular user and detachably connected to the processing device."

Therefore, because Sims does not disclose or suggest all the limitations of independent Claims 1, 25, 32, 38, and 44, Claims 1, 25, 32, 38, and 44 are patentable over Sims.

Claims 2-7 and 9-24 are dependent on Claim 1, Claims 26-29 and 31 are dependent on Claim 25, Claims 35-37 are dependent on Claim 32, Claims 40-43 are dependent on Claim 38, and contain additional limitations that further distinguish them from Sims. Therefore, Claims 2-7, 9-24, 26-29, 31, 35-37, and 40-43 are patentable over Sims for at least the same reasons stated above with regard to Claims 1, 25, 32, and 38.

Rejection Under 35 U.S.C. § 103(a)

Claim 18 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Sims in view of Keeler, jr. et al. (U.S. Patent No. 6,502,130, hereinafter "Keeler").

Keeler is directed toward a "system and method which collects dynamic connectivity data from an area network interconnecting multiple computing devices" (Keeler, Abstract) and does not remedy the deficiencies of Sims noted above. Claim 18 is also dependent on Claim 1 and contains additional limitations that further distinguish it from Sims in view of

v1   -13-   Serial No. 09/760,956

Keeler. Therefore, because neither Sims nor Keeler, alone or in combination, disclose or suggest all the limitations of Claim 18, Claim 18 is patentable over Sims in view of Keeler for at least the same reasons stated above with respect to Claim 1.

v1

-14-

Serial No. 09/760,956

CONCLUSION

For the above reasons, Applicant believes pending Claims 1-7, 9-29, 31-32, 35-38, and 40-44 are now in condition for allowance and allowance of the application is hereby solicited. If the Examiner has any questions or concerns, the Examiner is hereby requested to telephone Applicants' Attorney at (949) 752-7040.

Respectfully submitted,

Certificate of Transmission

I hereby certify that this correspondence is being facsimile transmitted to the Commissioner for Patents. Fax No. 703-872-9306 on the date stated below.

Tina Kavanaugh   November 24, 2004

David S. Park
Attorney for Applicant(s)
Reg. No. 52,094

LAW OFFICES OF
MacPHERSON KWOK
CHEN & HEID LLP

2400 MICHELSON DR.
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

v1   -15-   Serial No. 09/760,956

PAGE 18/18 * RCVD AT 11/24/2004 3:41:59 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/6 * DNIS:8729306 * CSID:9497527049 * DURATION (mm-ss):05-28